

Застосування технології блокчейну для забезпечення автентичності доказів

Сергій Коломійцев

науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі, навчально-науковий інститут № 4, Харківський національний університет внутрішніх справ МВС України, м. Харків, Україна, ORCID: <https://orcid.org/0009-0006-7070-9471>, e-mail: girbest@gmail.com

Андрій Синжерян

курсант навчально-наукового інституту № 4, Харківський національний університет внутрішніх справ МВС України, м. Харків, Україна, ORCID: <https://orcid.org/0009-0001-6063-4254>, e-mail: razorboyone@gmail.com

Іван Цуркан

курсант навчально-наукового інституту № 4, Харківський національний університет внутрішніх справ МВС України, м. Харків, Україна, ORCID: <https://orcid.org/0009-0009-6621-4056>, e-mail: curivan82@gmail.com

Технологія блокчейну забезпечує надійне зберігання цифрових доказів завдяки децентралізації, незмінності та прозорості. Її застосування в судово-експертній діяльності гарантує автентичність даних і захищає від маніпуляцій.

Ключові слова: блокчейн; цифрові докази; автентичність; судова експертиза.

Using Blockchain Technology to Ensure Evidence Authenticity

Serhii Kolomiitsev, Andrii Synzherian, Ivan Tsurkan

Blockchain technology offers secure storage of digital evidence due to its decentralization, immutability, and transparency. Its application during forensic activities guarantees data authenticity and safeguards against manipulation.

Keywords: blockchain; digital evidence; authenticity; forensic examination.

Блокчейн [1] — це технологія зберігання інформації, яка працює як цифровий реєстр або база даних. Технологія блокчейну децентралізована, тобто інформація зберігається не на одному сервері, а на багатьох комп'ютерах (вузлах), які підтримують роботу мережі. Це означає, що жоден окремий користувач або організація не контролює всі дані, і будь-які

спроби маніпуляції одразу виявлять інші учасники мережі. Децентралізація робить блокчейн стійким до зломів і втрат даних, оскільки система продовжує працювати, навіть якщо кілька вузлів виходять з ладу.

Уся інформація у блокчейні зберігається у вигляді блоків, кожен з яких містить певні дані. Блоки пов'язані між собою у хронологічному порядку, утворюючи ланцюг (англ. *chain*). Основною особливістю блокчейну є те, що, коли блок додається до ланцюга, його неможливо змінити або видалити без зміни всіх наступних блоків. Кожен блок містить кілька елементів: дані, хеш [2] попереднього блоку та власний унікальний хеш. Хеш — це криптографічний код, який генерується на основі вмісту блоку. Якщо вміст блоку змінюється навіть незначно, хеш також змінюється, що одразу виявляє маніпуляції з даними. Унаслідок цього блокчейн є надійним і захищеним від підробок способом зберігання даних.

Завдяки ключовим характеристикам — незмінності, прозорості, децентралізації та хронологічній фіксації — блокчейн може суттєво змінити підхід до забезпечення автентичності доказів у судово-експертній діяльності.

Об'єкти досліджень у вигляді фотографій, відеоматеріалів або документів, зібрані органами досудового слідства під час проведення відповідних слідчих дій, після комп'ютерної обробки у вигляді файлів можуть бути завантажені у блокчейн і кожен такий файл може бути перетворений

у хеш. Цей хеш фіксується у блокчейні. Якщо будь-яка частина файлу буде змінена (навіть на один біт), хеш також зміниться, сигналізуючи про підробку. У такий спосіб блокчейн гарантує, що жоден із збережених об'єктів досліджень не може бути змінений після його реєстрації. Це дасть змогу сторонам процесу (обвинуваченню, захисту, суду) упевнитися, що у процесі проведення експертних досліджень жоден з наданих об'єктів не було навмисно піддано змінам після їх виявлення та вилучення під час проведення слідчих дій.

Блокчейн підтримує можливість збереження даних у зашифрованому вигляді. Хоча самі дані можуть бути конфіденційними й недоступними для публічного перегляду, їхні хеші зберігаються відкрито. Так, висновки судово-медичних експертиз, витяги із історії захворювань, результати комп'ютерної томографії, інша медична документація особистого характеру, а також аналіз ДНК, можуть бути зашифровані та збережені у блокчейні для захисту приватності. Водночас хеш даних і час їх додавання будуть доступні для перевірки, що забезпечує збереження автентичності.

Блокчейн точно фіксує час (англ. *timestamp*) додавання нових даних у систему, що дає змогу органам досудового слідства не тільки зберігати виявлені докази, а й точно визначати, коли саме їх зібрали й завантажили у базу даних.

Технологія блокчейну може стати важливим інструментом для судових експертів і слідчих органів, особливо

в добу цифровізації. Вона гарантує незмінність, прозорість і надійність збереження цифрових доказів, забезпечує їхню автентичність і правильне застосування у судових процесах. Це особливо актуально у резонансних справах для виключення можливості умисного впливу на доказову базу та для винесення обґрунтованого судового рішення.

Перелік джерел посилання

1. What is blockchain? / IBM. URL: <https://www.ibm.com/topics/blockchain> (дата звернення: 02.10.2024).
2. Hash Function / NIST. URL: https://csrc.nist.gov/glossary/term/hash_function (дата звернення: 02.10.2024).